Comments Received on SP 800-152

Date: 1/10/14
From: Kramer, Timothy <tim.kramer@navy.mil>:

Section 2.10 in the draft SP 800-152 discusses computers as part of a FCKMS. Would it be advisable to require that they be dedicated computers?

For Section 5 ("Roles and Responsibilities") and others, is it possible to require that definition of responsibilities in the CKMS include any requirements defined in the Security Policies for the specific FIPS-approved products employed? An example of this would be where certain products' Security Policies require daily (or weekly, or monthly) inspection of TELs by the Cryptographic Officer or IAM. In most cases, this requirement is ignored because it's not "brought forward" into local policy, procedures, and/or accreditation documentation.

V/R,
Tim Kramer

From: <Harris>, "Michael W. (CDC/OCOO/OCIO)" <fnb0@cdc.gov>
Date: Thursday, February 27, 2014 8:20 AM

CDC has no comments to provide on the *draft Special Publication (SP) 800-152, A Profile for U.S. Federal Cryptographic Key Management Systems*.

Thank you for the opportunity to review and comment.

Thanks,

Michael W. Harris, CISSP, Information Technology Specialist, Office of the Chief Information Security Officer (OCISO), Centers for Disease Control and Prevention (CDC)

From: <Ford>, Stephen <Stephen.Ford@fda.hhs.gov>
Date: Wednesday, March 5, 2014 1:35 PM

There are two PR:10.1 one on pg 111, and one on pg 112.

Stephen Ford
Architecture & Engineering Team
Security Branch , Division of Technology
Administration

Office of Information M

From: <Burns>, Robert <Robert.Burns@thalesesec.com>
Date: Wednesday, March 5, 2014 2:48 PM

Attached you will find Thales e-Security's consolidated comments regarding the proposed NIST SP800-152 standard.

If you require any additional information or clarification on our comments, please feel free to contact me at the email address and/or phone number below.

Thanks,

Bob

CLASSIFICATION : Thales e-Security OPEN

Robert Burns
Security Principal, Office of the CTO
THALES Information Systems Security

#	Organi-zation	Type	Reference	Comment(Include rationale for comment)	Suggested change
1	2	E	Page 28, First Sentence	Acronym "FCKS" is used for the first time in the document; suspect it should be "FCKMS" instead.	Replace with FCKMS.
2	2	E	Page 44, First Paragraph	Recommendation to rotate roles periodically across individuals to limit long-term abuse seems to ignore the more tangible risk of human error introduced by users unfamiliar with their current role.	Provide additional justification for this recommendation. Alternatively ensure sensitive roles are performed multiple individuals (e.g. a quorum) to limit long-term abuse instead.
3	2	E	Page 45, PA:5.2	Recommendation to rotate roles periodically across individuals to limit long-term abuse seems to ignore the more tangible risk of human error introduced by users unfamiliar with their current role.	Recommend replacing role rotation with quorum based roles to minimize long-term abuse.
4	2	T	Page 48, item p)	Although key usage (e.g. number of times a key is used) is a useful metric, there are often many other counters associated with key usage, such as encryption byte counts for evaluating key crypto period irrespective of key expiration dates.	Consider an additional metric for tracking number of bytes encrypted by the key.
5	2	T	Page 59, PR:6.28	Destruction of all the key metadata contradicts NIST SP800-57 Part 1 (Rev 3), Section 8.4 which indicates that metadata retention may be required to support audit requirements. For example, to support a future discovery of key compromise, it may be necessary to know the key lifecycle, amount, and types of data the key was protecting to assess exposure.	Change PR:6.28 to refer only to the key, not the metadata. Create a separate requirement to guide the management and retention of the key metadata in the destruction phase.

From: Chuck White <cwhite@semper-fortis.com>
Date: Wednesday, March 5, 2014 3:14 PM

On Interoperability:

In respect for comments for Interoperability I think it would be better language to say that "Interoperability should be considered for cryptographic algorithms, as well as FCKMS **management** commands"

Also it is important to have an industry focus on interoperability – ie OASIS KMIP, and a USG focus on security - ie NIST 800-53, etc. But it is important to point out where to look in industry so folks have an idea of where to start.

Interoperability needs to be expanded to more than just encryption algorithms it also needs to incorporate the operations associated with Cryptographic Key Management not just the algorithms. From an industry perspective, standards such as Key Management Interoperability Protocol provide an industry based framework for managing Key Management infrastructure.

Agreeing on algorithms is important, agreeing on protocols for management operations is of equal importance to enforce adoption.

Using a car example – the algorithm is the engine, the management operations represent the transmission or steering wheel – it's how you make the FCKMS available for folks to use that will drive adoption.

On Logical vs Physical separation to controls:

Definitely want to look at things like PR 2.10, PR 6.2, PR 10.5 PR 6.8, PR 8.1, PF 6.13, and see if separation of physical and logical security controls. This is also has implications in defining Domains. This was a point of what happens for a FCKMS working on multiple domains was a logical concern vs a physical concern.

From a security professional perspective a physical control has a "Guns, Gates, and Guards" connotation, whereas controls on a piece of computing technology is still a logical control. This has implications on evaluating FCKMS based on the end results of the profile defined in NIST SP800-152.

Thanks!

Chuck

Charles White
CTO
Semper Fortis Solutions, LLC
14840 Conference Center Drive, Suite Y
Chantilly, VA 20151

From: "tspann@aegisolve.com" <tspann@aegisolve.com>
Date: Wednesday, March 5, 2014 5:25 PM

Thanks for a very productive and informative FCKMS workshop. Please allow me to comment as follows:

Regarding SP800-152, PR:8.14. "A Federal CKMS shall use cryptographic modules in accordance with the security policy of that module."

For a cryptographic module that has been validated before Dec. 31, 2013...it may be beneficial to add a requirement that the security policy has been updated to address the algorithm transition timelines of SP800-131A and re-validated by CMVP.

This would help to ensure that a given security policy contains sufficient details regarding the appropriateness of services and security functions as per SP800-131A available in the Approved mode of operation.

Consider including a requirement that the Approved algorithm(s) used for firmware load test must have a minimum of 112-bits of equivalent computational resistance to attack.

Sincerely,

Travis Spann | ÆGISOLVE, INC.

From: "Brych,Chris" <Chris.Brych@safenet-inc.com>
Date: Thursday, March 13, 2014 3:15 PM

It was a pleasure meeting you all at the NIST Key Management Workshop last week. Below are some additional feedback I had from discussions at the NIST key management workshop last week in Gaithersburg.

1. Page 104 PA: 9.3:
   Non-cryptographic software and hardware used within a Federal CKMS **should** be validated using the Common Criteria Standard ([ISO/IEC 15408 Parts 1- 3], National Information Assurance Partnership(NIAP)). I believe that a reference to a NIAP Approved Protection Profile should be made to provide clarity. Currently there is no "Approved" Protection Profile for a key management system. This is an excellent opportunity to approach NIAP to specify a need for a FCKMS protection profile. The requirements defined in 800-152 is a good start in defining requirements for a FCKMS.

2. Page 120: 11.1.1 Review of Third-Party Testing and Verification of Test Results. Again referencing need for NIAP CC evaluation. See item 1 above for action.

3. Page 85: Interoperability. As part of Interoperability requirements a FCKMS, specification of the "Allowed" cryptographic protocols allowed for key distribution/establishment, a FCKMS shall support the following protocols and certified against FIPS PUB 140-2:

   - TLS 1.2
   - IPSEC
   - SSH V2
   - SNMP V3

   The intent for specifying supported protocols is so that we don't leave it to vendors to guess which security protocols to be implemented which could pose interoperability challenges within the key management system. It is also implied that these cryptographic protocols be used in conjunction with the KMIP protocol.

4. PR 2.12, Page 21: Recommend changing the requirement that states " at the high impact level, Federal CKMS shall employ cryptographic modules validated at FIPS 140 security Level 4" to "at the high impact level, Federal CKMS shall employ cryptographic modules validated at FIPS security Level 3 Overall with Physical Security Requirements validated at FIPS Level 4 requirements." The reason for this is that all of the FIPS Level 4 modules validated to date only include the boot loader code as part of their evaluation providing little to no validated functionality. The reason vendors have done this is because of the exhaustive formal model requirements that FIPS Level 4 requires that make validating the entire firmware functionality near impossible to certify. By accepting a FIPS 140 Level 3 Overall certified module with FIPS Level 4 Physical Security Requirements provides the added Firmware functionality while also providing that extra level of physical protection required for protecting high impact level data.

Regards,

Chris

From: John Leiseboer
Date: Tuesday, 4 March 2014 9:17 AM
John Leiseboer
CTO, QuintessenceLabs

1. Use and Design of CKMS RNG(s)

The FCKMS profile says very little about the RNG used to create random numbers, and generate keys, in the CKMS. It can be assumed that an approved RNG shall be used, but there are no requirements on how the RNG shall be designed, or used.

NIST SP 800-90A DRBGs provide a number of inputs, including seed input, and personalization strings. If a CKMS supports a single (pseudo) RNG instance, then it is possible that all keys generated by the CKMS are derived from RNG output generated from the same input parameters. If the input parameters can be controlled by a single user, administrative, or otherwise, then that single user can predict key values generated from the RNG output.

It may be desirable to specify that independent instantiations of RNGs, with different seed inputs, and optionally different personalization strings, or that a non-deterministic, true RNG, be used for each key generated by the CKMS.

2. FR: 6.13

This requirement states that the RNG used shall be specified for each key type. I assume that this means the RNG type, rather than a specific RNG instance. If known, shouldn't the RNG instance also be specified? If it is discovered at some point in time that a specific instance of an RNG was faulty, or compromised, then knowing the instance would help to identify any keys that may have been generated using the RNG output.

John Leiseboer